A limit on nonlocality in any world in which communication complexity is not trivial

Gilles Brassard[1], Harry Buhrman[2,3], Noah Linden[4]
André Allan Méthot[1], Alain Tapp[1] and Falk Unger[3]

1. *Département IRO, Université de Montréal, Canada*
{brassard, methotan, tappa}@iro.umontreal.ca

2. *ILLC, Universiteit van Amsterdam, The Netherlands*

3. *Centrum voor Wiskunde en Informatica (CWI), Amsterdam, The Netherlands*
{harry.buhrman, falk.unger}@cwi.nl

4. *Department of Mathematics, University of Bristol, United Kingdom*
n.linden@bristol.ac.uk

4 August 2005

Abstract

Bell proved that quantum entanglement enables two space-like separated parties to exhibit classically impossible correlations. Even though these correlations are stronger than anything classically achievable, they cannot be harnessed to make instantaneous (faster than light) communication possible. Yet, Popescu and Rohrlich have shown that even stronger correlations can be defined, under which instantaneous communication remains impossible. This raises the question: Why are the correlations achievable by quantum mechanics not maximal among those that preserve causality? We give a partial answer to this question by showing that slightly stronger correlations would result in a world in which communication complexity becomes trivial.

Keywords: Nonlocality; Communication complexity; Bell inequalities; Foundations of quantum mechanics.

1 Introduction

In the field of quantum information processing, entanglement can be harnessed to accomplish amazing feats, such as quantum teleportation [1]. The first proof that genuinely nonclassical behaviour could be produced by quantum-mechanical devices was given by John Bell in 1964 [2], when he proved that quantum entanglement enables two space-like separated parties to exhibit correlations that are stronger than anything allowed by classical physics. A few years later, John Clauser, Michael Horne, Abner Shimony and Richard Holt (CHSH), inspired by the work of Bell, proposed another inequality [3], which was easier to translate into a feasible experiment [4, 5] to test local hidden-variable theories. Their proposal fits nicely into the more modern framework of nonlocal boxes, introduced by Sandu Popescu and Daniel Rohrlich [6, Eq. (7)].

A *nonlocal box* (NLB) is an imaginary device that has an input-output port at Alice's and another one at Bob's, even though Alice and Bob can be space-like separated. Whenever Alice feeds a bit x into her input port, she gets a uniformly distributed random output bit a, locally uncorrelated with anything else, including her own input bit. The same applies to Bob, whose input and output bits we call y and b, respectively. The "magic" appears in the form of a correlation between the pair of outputs and the pair of inputs: the exclusive-or (sum modulo two, denoted "$\oplus$") of the outputs is always equal to the logical AND of the inputs: $a \oplus b = x \wedge y$. Much like the correlations that can be established by use of quantum entanglement, this device is atemporal: Alice gets her output as soon as she feeds in her input, regardless of if and when Bob feeds in *his* input, and vice versa. Also inspired by entanglement, this is a *one-shot* device: the correlation appears only as a result of the first pair of inputs fed in by Alice and Bob, respectively. Of course, they can have more than one NLB at their disposal, which is then seen as a *resource* of a different nature than entanglement [7].

A crucial property of NLBs is that they cannot be used by Alice and Bob to signal instantaneously (faster than light) to one another. This is because the outputs that can be observed are purely random from a local perspective. In other words, NLBs are nonlocal, yet they are *causal*: they cannot make an effect precede its cause in the context of special relativity. We are interested in the question of how well the correlation of NLBs can be *approximated* by devices that follow the laws of physics.

Even though originally presented in different terms, it is easy to recast the CHSH inequality in the language of imperfect NLBs. The availability of prior shared entanglement allows Alice and Bob to approximate NLBs with a success probability equal to

$$\wp = \cos^2 \tfrac{\pi}{8} = \tfrac{2+\sqrt{2}}{4} \approx 0.854\,.$$

This can be used to test local hidden-variable theories because it follows also from CHSH that no local realistic (classical) theory can succeed with probability greater than $^3/_4$ if Alice and Bob are space-like separated. Later, Boris Tsirelson proved the optimality of the CHSH inequality, which translates into saying that quantum mechanics does not allow for a success probability greater than $\wp$ at the game of simulating NLBs [8]. See also [9] for an information-theoretic proof of the same result.

The questions of interest in this paper are: (1) *Considering that perfect NLBs would not violate causality, why do the laws of quantum mechanics only allow us to implement NLBs better than anything classically possible, yet not perfectly?*; and (2) *Why do they provide us with an approximation of NLBs that succeeds with probability $\wp$ rather than something better?*

Before we can pursue this line of thought further, we need to review briefly the field of (*quantum*) *communication complexity* [10, 11, 12, 13]. Assume Alice and Bob wish to compute some Boolean function $f(x, y)$ of input x, known to Alice only, and input y, known to Bob only. Their concern is to minimize the amount of (classical) communication required between them for Alice to learn the answer. It is clear that this task cannot be accomplished without at least *some* communication (even if Alice and Bob share prior entanglement), unless $f(x, y)$ does not actually depend on y, because otherwise instantaneous signalling would be possible. Thus, we say that the communication complexity of f is *trivial* if the problem can be solved with a *single bit* of communication.

It is known that prior entanglement shared between Alice and Bob helps sometimes but not always. Some functions can be computed with exponentially less communication than would have been required in a purely classical world [14]. Yet other functions, such as the *inner product*, require as many bits to be communicated as the length of Bob's input, whether or not prior entanglement is available [15]: those are not trivial. Surprisingly, Wim van Dam [16], and independently Richard Cleve [17], proved that the availability of perfect NLBs makes the communication complexity of *all*

Boolean functions trivial! This answers the first question above: If we take as an axiom that communication complexity should not be trivial in the real world, it had to be impossible for quantum mechanics to provide a perfect implementation of NLBs. Indeed, most computer scientists would consider a world in which communication complexity is trivial to be as surprising as a modern physicist would find the violation of causality.

In order to answer the second question, we turn our attention to the *probabilistic* version of communication complexity, in which we do not require Alice to learn the value of $f(x, y)$ with certainty. Instead, we shall be satisfied if she can obtain an answer that is correct with a probability bounded away from $^1/_2$. In other words, there must exist some real number $p > {}^1/_2$ such that the probability that Alice guesses the correct value of $f(x, y)$ is at least p for *all* pairs (x, y) of inputs. Here, the probability is taken over possible probabilistic behaviour at Alice's and Bob's, as well as over the value of random variables shared between Alice and Bob. Note that there is no need for Boolean shared random variables if prior entanglement or perfect NLBs is available since either one of those resources can be used by Alice and Bob to obtain identical yet random coin tosses.

When we extend the notion of "trivial" communication complexity to fit this probabilistic framework, the computation of the inner product remains nontrivial according to quantum mechanics: Even if Alice and Bob share prior entanglement, they need to transmit at least $\max(\frac{1}{2}(2p-1)^2, (2p-1)^4)n - \frac{1}{2}$ classical bits in order to succeed with probability at least $p > {}^1/_2$, which is linear in the length n of the inputs when p is a constant [15]. Our main theorem, stated below and proven in Section 3, provides a partial answer to the second question.

Theorem 1. *In any world in which it is possible, without communication, to implement an approximation to the NLB that works correctly with probability greater than* $\frac{3+\sqrt{6}}{6} \approx 90.8\%$, every *Boolean function has trivial probabilistic communication complexity.*

To prove this theorem, we introduce the notion of *distributed computation* and the notion of *bias* for such computations. Then, we show how to amplify the natural bias of *any* Boolean function by having Alice and Bob calculate it many times and taking the majority. We determine how imperfect a majority gate can be and still increase the bias. Finally, we construct a majority gate

with the use of NLBs, and we determine to what extent we can allow *them* to be faulty.

2 Preliminary Definitions and Lemmas

Definition 1. A bit c is *distributed* if Alice has bit a and Bob bit b such that $c = a \oplus b$.

Definition 2. A Boolean function f is *distributively computed* by Alice and Bob if, given inputs x and y, respectively, they can produce a distributed bit equal to $f(x,y)$. Communication is not allowed during a distributed computation.

Definition 3. A Boolean function is *biased* if it can be distributively computed with probability strictly greater than $^1/_2$.

Lemma 1. Provided Alice and Bob are allowed to share random variables, *all* Boolean functions are biased.

Proof. Let f be an arbitrary Boolean function and let Alice and Bob share a uniformly distributed random variable z of the same size as Bob's input y. (It is usual practice in communication complexity [10] to assume that each party knows the size of both inputs.) Upon receiving her input x, Alice produces $a = f(x,z)$. Bob's strategy is to test if $y = z$. If so, he produces $b = 0$; if not, he produces a uniformly distributed random bit b. In the lucky event that $y = z$, the bit distributed between Alice and Bob is correct since $a \oplus b = f(x,z) \oplus 0 = f(x,y)$. This happens with probability 2^{-n} if n is the size of Bob's input. In all other cases (with overwhelming probability $1 - 2^{-n}$), the distributed bit $a \oplus b$ is uniformly random, hence it is correct with probability $^1/_2$. Summing up, the distributed bit is correct with probability

$$\Pr[a \oplus b = f(x,y)] = \frac{1}{2^n} + \Big(1 - \frac{1}{2^n}\Big)\frac{1}{2} = \frac{1}{2} + \frac{1}{2^{n+1}}\,,$$

which is indeed strictly greater than $^1/_2$. □

Definition 4. A Boolean function has *bounded bias* if it can be distributively computed with probability bounded away from $^1/_2$.

Remark 1. The difference between bias and *bounded* bias is that the probability of being correct in the former case can come arbitrarily close to $^1/_2$ as the size of the inputs increases. In the latter case, there must be some fixed $p > {^1/_2}$ such that the probability of being correct is at least p no matter how large the inputs are.

Lemma 2. Any Boolean function that has bounded bias has trivial probabilistic communication complexity.

Proof. Assume Boolean function f has bounded bias. For all inputs x and y, Alice and Bob can produce bits a and b, respectively, without communication, such that $a \oplus b = f(x,y)$ with probability at least $p > {^1/_2}$. If Bob sends b to Alice, she can compute $a \oplus b$, which is equal to $f(x,y)$ with bounded error probability, after a single bit has been communicated. □

Definition 5. The *nonlocal majority* problem consists in computing the distributed majority of three distributed bits. More precisely, let Alice have bits x_1, x_2, x_3 and Bob have y_1, y_2, y_3. The purpose is for Alice and Bob to compute a and b, respectively, such that

$$a \oplus b = \mathrm{Maj}(x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3)\,,$$

where $\mathrm{Maj}(u,v,w) = \lfloor (u+v+w)/2 \rfloor$ denotes the most frequent bit among u, v and w. The computation of a and b must be achieved without any communication between Alice and Bob.

John von Neumann proved a statement rather similar to Lemma 3 below in 1956, but in the context of ordinary circuits rather than distributed computation [18]. We sketch the proof nevertheless for the sake of completeness.

Lemma 3. For any q such that ${^5/_6} < q \le 1$, if Alice and Bob can compute nonlocal majority with probability at least q, every Boolean function has bounded bias.

Proof. Let f be an arbitrary Boolean function, fix Bob's input size, and consider any $p > {^1/_2}$ so that Alice and Bob can distributively compute f with probability at least p. We know from Lemma 1 that such a p exists (although it can depend on the size of the inputs). Let Alice and Bob apply their distributed computational process three times, with independent random choices and shared random variables each time. This produces three

distributed bits such that each of them is correct with probability at least p. Let now Alice and Bob compute the nonlocal majority of these three outcomes with probability at least q that the nonlocal majority be computed correctly. Because the overall result will be correct either if most of the distributed outcomes were correct and the distributed majority calculation was performed correctly, or if most of the distributed outcomes were wrong and the distributed majority calculation was performed incorrectly, the probability that the distributed majority as computed yields the correct value of f is

$$h(p) = q(p^3 + 3p^2(1-p)) + (1-q)(3p(1-p)^2 + (1-p)^3)\,.$$

Define

$$\delta = q - {}^5\!/_6 > 0 \quad \text{and} \quad s = \frac{1}{2} + \frac{3\sqrt{\delta}}{2\sqrt{1+3\delta}} > \frac{1}{2}\,.$$

It can be shown that $p < h(p) < s$ provided ${}^1\!/_2 < p < s$. Because of this and the fact that $h(p)$ is continuous over the entire range ${}^1\!/_2 < p < s$, iteration of the above process can boost the probability of distributively computing the correct answer arbitrarily close to s. This proves that f has bounded bias because, given any fixed value of $q > {}^5\!/_6$, we can choose an arbitrary constant $t < s$ such that $t > {}^1\!/_2$ and distributively compute f with probability at least t of being correct, independently of the size of the inputs. $\square$

Definition 6. The *nonlocal equality* problem consists in distributively deciding if three distributed bits are equal. More precisely, let Alice have bits x_1, x_2, x_3 and Bob have y_1, y_2, y_3. The purpose is for Alice and Bob to compute a and b, respectively, such that

$$a \oplus b = \begin{cases} 1 & \text{if } x_1 \oplus y_1 = x_2 \oplus y_2 = x_3 \oplus y_3 \\ 0 & \text{otherwise}\,. \end{cases}$$

The computation of a and b must be achieved without any communication between Alice and Bob.

Lemma 4. Nonlocal equality can be computed using only two (perfect) nonlocal boxes.

Proof. The goal is to obtain a and b such that:

$$a \oplus b \;=\; (x_1 \oplus y_1 = x_2 \oplus y_2) \wedge (x_2 \oplus y_2 = x_3 \oplus y_3). \tag{1}$$

First, Alice and Bob compute locally

$$x' = \overline{x_1} \oplus x_2, \quad y' = y_1 \oplus y_2, \quad x'' = \overline{x_2} \oplus x_3 \quad \text{and} \quad y'' = y_2 \oplus y_3 \,.$$

Then (1) becomes equivalent to $(x' \oplus y') \wedge (x'' \oplus y'') = a \oplus b$. So, it is sufficient to show how Alice and Bob can compute the AND of the distributed bits $x' \oplus y'$ and $x'' \oplus y''$.

By the distributivity law of the AND over the exclusive-or, we have

$$(x' \oplus y') \wedge (x'' \oplus y'') = (x' \wedge x'') \oplus (x' \wedge y'') \oplus (x'' \wedge y') \oplus (y' \wedge y'') \,.$$

Using two nonlocal boxes, Alice and Bob can compute distributed bits $a' \oplus b'$ and $a'' \oplus b''$ with $a' \oplus b' = x' \wedge y''$ and $a'' \oplus b'' = x'' \wedge y'$. Setting $a = (x' \wedge x'') \oplus a' \oplus a''$ and $b = (y' \wedge y'') \oplus b' \oplus b''$ yields (1), as desired. □

Lemma 5. Nonlocal majority can be computed using only two (perfect) nonlocal boxes.

Proof. Let x_1, x_2, x_3 be Alice's input and y_1, y_2, y_3 be Bob's. For $i \in \{1, 2, 3\}$, let $z_i = x_i \oplus y_i$ be the i^{th} distributed input bit. By virtue of Lemma 4, Alice and Bob use their two NLBs to compute the nonlocal equality of their inputs, yielding a and b so that $a \oplus b = 1$ if and only if z_1, z_2 and z_3 are equal. Finally, Alice produces $a' = \overline{a} \oplus x_1 \oplus x_2 \oplus x_3$ and Bob produces $b' = b \oplus y_1 \oplus y_2 \oplus y_3$. Let

$$z = a' \oplus b' = (\overline{a} \oplus b) \oplus (z_1 \oplus z_2 \oplus z_3)$$

be the distributed bit computed by this protocol. Four cases need to be considered, depending on the number ℓ of 1s among the z_i's:

1. if $\ell = 0$, then $a \oplus b = 1$ and $z_1 \oplus z_2 \oplus z_3 = 0$;
2. if $\ell = 1$, then $a \oplus b = 0$ and $z_1 \oplus z_2 \oplus z_3 = 1$;
3. if $\ell = 2$, then $a \oplus b = 0$ and $z_1 \oplus z_2 \oplus z_3 = 0$;
4. if $\ell = 3$, then $a \oplus b = 1$ and $z_1 \oplus z_2 \oplus z_3 = 1$.

We see that $z = 0$ in the first two cases and $z = 1$ in the last two, so that $z = \mathrm{Maj}(z_1, z_2, z_3)$ in all cases. □

We are now ready to prove our main theorem.

3 Proof of the Main Theorem

Before proving it, let us repeat the statement of the main theorem.

Theorem 1. *In any world in which it is possible, without communication, to implement an approximation to the NLB that works correctly with probability greater than* $\frac{3+\sqrt{6}}{6} \approx 90.8\%$, every *Boolean function has trivial probabilistic communication complexity.*

Proof. Assume NLBs can be approximated with some probability p of yielding the correct result. Using them, we can compute nonlocal majority with probability $q = p^2 + (1-p)^2$ since the protocol given in the proof of Lemma 5 succeeds precisely if none or both of the NLBs behave incorrectly. The result follows from Lemmas 2 and 3 because $q > {}^5\!/_6$ whenever $p > \frac{3+\sqrt{6}}{6} \approx 0.908$. A more precise calculation, based on the proof of Lemma 3, shows that the two-party computation of *any* Boolean function can be achieved using a single bit of communication, with a probability of correct answer arbitrarily close to

$$\frac{1}{2} + \frac{\sqrt{3p^2 - 3p + {}^1\!/_4}}{2p-1}$$

provided $p > \frac{3+\sqrt{6}}{6}$, making it trivial by definition. □

Corollary 1. In any world in which probabilistic communication complexity is nontrivial, nonlocal boxes cannot be implemented without communication, even if we are satisfied in obtaining the correct behaviour with probability $\frac{3+\sqrt{6}}{6} \approx 90.8\%$.

Remark 2. Neither nonlocal majority nor nonlocal equality can be solved exactly with a single nonlocal box. Otherwise, entanglement could approximate that NLB well enough to solve the nonlocal majority problem with probability $\wp \approx 0.854 > {}^5\!/_6$ of being correct [3]. It would follow from Lemmas 2 and 3 that all Boolean functions have trivial probabilistic communication complexity according to quantum mechanics. But we know this not to be the case, in particular for the inner product [15].

Remark 3. Our results also give bounds on the maximum admissible error for elementary gates in fault-tolerant circuits: In the proof of Lemma 4, we show how to simulate distributed AND-gates. Using NLBs with the

(quantum-mechanically achievable) correctness probability $\wp$, such a distributed AND is correct with probability $(1-\wp)^2 + \wp^2 = {}^3\!/_4$. Furthermore, a distributed NOT-gate on a distributed bit can be implemented perfectly if just one party (say Alice) negates her bit. Like any other Boolean function, the inner product $IP(x,y) = \bigoplus_i (x_i \wedge y_i)$ can be computed using only AND and NOT gates. But the entanglement-assisted communication complexity of IP is in $\Omega(n)$. Thus, if we allow Alice and Bob to communicate only a constant number of bits but allow them to use an arbitrary number of NLBs (with correctness $\wp$), they still cannot compute the inner product function for arbitrary inputs.

It follows that no family of circuits, consisting solely of (perfect) NOT-gates and AND-gates that independently fail with probability at most ${}^1\!/_4$, can compute the inner product function for arbitrary input sizes. A stronger result along these lines had already been proven by William Evans and Nicholas Pippenger [19], but their purely classical proof is significantly more complicated.

4 Conclusions

In conclusion, we have shown that in any world in which communication complexity is nontrivial, there is a bound on how much Nature can be non-local. For this purpose, we developed a protocol to distributively compute with bounded bias any Boolean function, provided we can approximate non-local boxes with probability greater than $\frac{3+\sqrt{6}}{6} \approx 0.908$. This bound, which is an improvement over previous knowledge that nonlocal boxes could not be implemented exactly [16, 17], approaches the actual bound $\wp \approx 0.854$ imposed by quantum mechanics. The obvious open question is to close the gap between these probabilities. A proof that nontrivial communication complexity forbids nonlocal boxes to be approximated with probability greater than $\wp$ would be very interesting, as it would make Tsirelson's bound [8] inevitable. Conversely, if we could show how to use quantum entanglement to approximate nonlocal equality with probability ${}^5\!/_6$ of success, this would imply that our line of reasoning cannot be improved.

Acknowledgements

The authors are grateful to Richard Cleve for stimulating discussions. H.B., N.L. and F.U. thank the Newton Institute where part of this work was done. G. B. is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canadian Institute for Advanced Research (CIAR) and the Canada Research Chair Programme. H.B., N.L. and F.U. are supported by the EU under project RESQ (IST-2001-37559). H.B. and F.U. are supported also by the NWO vici project 2004-2009. A.T. is supported by NSERC, CIAR, the Mathematics of Information Technology and Complex Systems Network (MITACS) and the Fonds Québecois de Recherche sur la Nature et les Technologies (FQRNT).

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Physical Review Letters* **70**(13):1895–1899 (1993).

[2] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics* **1**(3):195–200 (1964).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical Review Letters* **23**(15):880–884 (1969).

[4] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories", *Physical Review Letters* **28**(14):938–941 (1972).

[5] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via Bell's theorem", *Physical Review Letters* **47**(7):460–463 (1981).

[6] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom", *Foundations of Physics* **24**(3):379–385 (1994).

[7] A. Broadbent and A. A. Méthot, "On the power of non-local boxes", preprint available at `http://arxiv.org/abs/quant-ph/0504136` (2005).

[8] B. S. Cirel'son, "Quantum generalizations of Bell's inequality", *Letters in Mathematical Physics* **4**(2):93–100 (1980).

[9] H. Buhrman, S. Massar, *Causality and Cirel'son bounds*, preprint available at `http://arxiv.org/abs/quant-ph/0409066` (2004)

[10] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, 1997).

[11] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Physical Review A* **56**(2):1201–1204 (1997).

[12] R. de Wolf, "Quantum communication and complexity", *Theoretical Computer Science* **287**(1):337–353 (2002).

[13] G. Brassard, "Quantum communication complexity", *Foundations of Physics* **33**(11):1593–1616 (2003).

[14] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation", *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), pp. 63–68.

[15] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, "Quantum entanglement and the communication complexity of the inner product function", *Proceedings of First NASA International Conference on Quantum Computing and Quantum Communication*, LNCS **1509** (Springer-Verlag, Heidelberg, 1998), pp. 61–74.

[16] W. van Dam, "Nonlocality & communication complexity", D.Phil. Thesis, University of Oxford, Chap. 9 (2000). See also "Implausible consequences of superstrong nonlocality", preprint available at `http://arxiv.org/abs/quant-ph/0501159` (2005).

[17] R. Cleve, personal communication.

[18] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components", *in Automata Studies* (C. E. Shannon and J. McCarthy, eds.), Princeton, 1956

[19] W. Evans and N. Pippenger, "On the Maximum Tolerable Noise for Reliable Computation by Formulas", *IEEE Transactions on Information Theory* **44**(3):1299–1305 (1998).